International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 3: March 2015, pp 1-4. www.aetsjournal.com ISSN (Online) : 2394-6237

Multimodal Biometrics System for Efficient Human Recognition

V.Prasathkumar, P.Jeevitha

Abstract— This paper presents a novel multi-level wavelet based fusion algorithm that combines information from fingerprint, face, iris, and signature images of an individual. The effectiveness of the fusion algorithm is experimentally validated by computing the matching scores and the equal error rates before fusion, after reconstruction of biometric images, and when the composite fused image is subjected to both frequency and geometric attacks. The complexity of the fusion and the reconstruction algorithms is O (n log n) and is suitable for many real-time applications. The final decision is made by fusion at "matching score level architecture" in which feature vectors are created independently for query images and are then compared to the enrollment templates which are stored during database preparation for each biometric trait. We also propose a multi-modal biometric algorithm that further reduces the equal error rate compared to individual biometric images. The proposed approach reduces the memory size, increases the recognition, accuracy using multi-modal biometric features, and withstands common attacks such as smoothing, cropping, and filtering due to tampering.

***Keywords*—** Novel multi-level wavelet based fusion algorithm, Fingerprint , Matching score level architecture , Biometric images etc.

I. INTRODUCTION

Biometrics" means "life measurement", but the term is usually associated with the use of unique physiological characteristics to identify an individual. One of the applications which most people associate with biometrics is security. It is an automated method of recognizing a person based on the features face, fingerprints, hand geometry, handwriting, iris, retinal, vein, voice etc. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

In particular, biometric authentication systems generally suffer from enrollment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition in certain environments. The algorithm includes all parts that are required for face and hand verification, such as feature extraction, classification and authentication. To find local facial features, such as eyes, mouth and nose, we apply a point distribution model and active shape models. We use the same system to find distinctive points in hand geometry.

V.PrasathKumar is Assistant Professor, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, India (e-mail: prasathkumar@ siet.ac.in).

P.Jeevitha is Assistant Professor, Sri Shakthi Institute of Engineering and Technology, Coimbatore, Tamilnadu, India (e-mail: prasathkumar@ siet.ac.in).

II. NECESSITY FOR MULTIMODEL BIOMETRICS

One way to overcome the problems in unimodal is the use of multi-biometrics. Driven by lower hardware costs, a multi biometric system uses multiple sensors for data acquisition.. Further, if the biometric trait being sensed or measured is noisy (a fingerprint with a scar or a voice altered by a cold, for example), the resultant matching score computed by the matching module may not be reliable. This problem can be solved by installing multiple sensors that capture different biometric traits. Such systems, known as multimodal biometric systems , are expected to be more reliable due to the presence of multiple pieces of evidence. These systems are also able to meet the stringent performance requirements imposed by various applications. For example, the feature extraction module of a fingerprint authentication system may be unable to extract features from fingerprints associated with specific individuals, due to the poor quality of the ridges. In such instances, it is useful to acquire multiple biometric traits for verifying the identity. Multimodal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously.

III. FACE RECOGNITION

Feature Extraction using EBGM and KDDA

A. Elastic Bunch Graph Matching (EBGM)

Face recognition using elastic bunch graph matching is based on recognizing novel faces by estimating a set of novel features using a data structure called a bunch graph. Similarly for each query image, the landmarks are estimated and located using bunch graph. Then the features are extracted by convolution with the number of instances of Gabor filters followed by the creation of face graph. The matching score (MS_{EBGM}) is calculated on the basis of similarity between face graphs of database and query image. The diagrammatic representation of EBGM algorithm is shown in Figure.

B. Kernel Direct Discriminant Analysis (KDDA)

Face recognition using KDDA is based on computation of feature space F (from training set) and projection of input pattern into the feature space to calculate significant discriminant features. For each of the *m* features in the database and *n* features in the query image, reference features

are chosen depending on the distance and rotation between the positions of features in the feature space. The matching score for each transformation of database and query feature vectors are calculated with respect to reference feature chosen using bounding box technique. MS_{KDDA} is defined by the maximum of all matching scores divided by the maximum number of features (among the query and the database).

C. Steps involved in face recognition

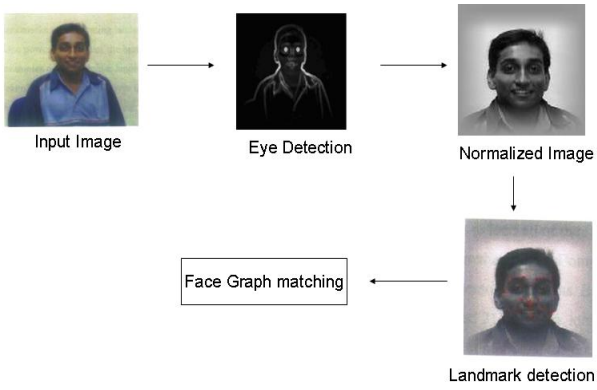

Fig 1: Combination of EBGM and KDDA

The matching scores from the above two classifiers are converted from distance to similarity score and are combined at matching score level using sum of score technique which significantly increases the accuracy of the face recognition system

IV. FINGERPRINT RECOGNITION

The fingerprint recognition system has been developed by the fusion of Reference Point and Minutiae Matching Techniques . The key steps involved are fingerprint enhancement, feature extraction using Reference point Algorithm and Minutiae Matching approach and computation of matching score. Feature Extraction using Reference point and Minutiae matching approach

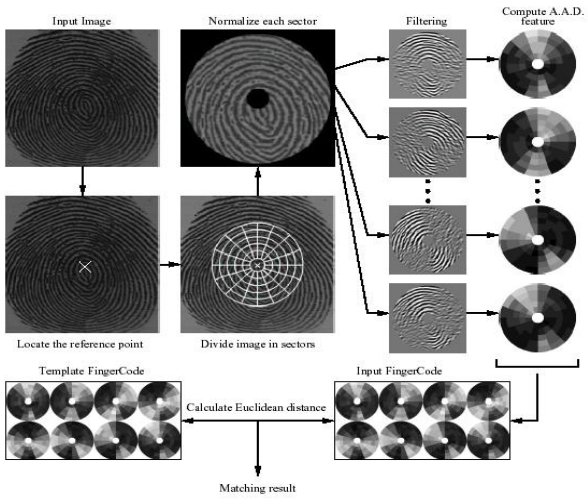

Fig 2: Diagrammatic representation of Reference point Location algorithm

A. Reference Point Algorithms

It gracefully handles local noise in a poor quality fingerprint. The detection should necessarily consider a large neighborhood in the fingerprint image. For an accurate localization of the reference point, the input image is segmented to remove any kind of noise present in the image. The Orientation Field is estimated along with the Y component. A specific pattern in which the value of Y-Component is maximum is Reference point (the point of maximum curvature). The finger code is generated by drawing concentric circles of fixed radius centered at reference point. The size of the feature vector is 512 values. The distance (D_{Ref}) for the database and query feature vectors is calculated using Euclidean distance method.

B. Minutiae Matching

The input fingerprint image is enhanced using Gabor Filters The enhanced image is further binarized and thinned using a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. The thinned image is used to detect minutiae points by locating ridge ending and bifurcations using Crossing Number (*CN*) method. The matching score MS_{MIN} between the database and query image is computed using Elastic matching approach.

C. Combination of Reference Point and Minutiae Matching Algorithm

The matching scores from the above two classifiers are converted from distance to similarity score and are combined at matching score level using sum of score technique which significantly increases the accuracy of the fingerprint system.

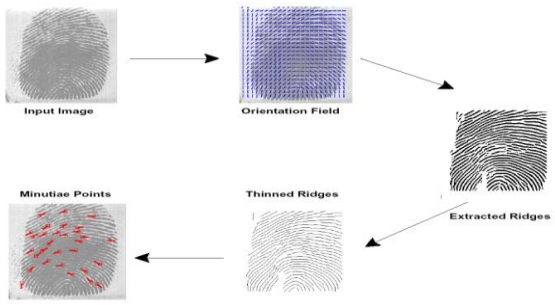

Fig 3: Steps involved in minutiae extraction

V. IRIS RECOGNITION

The iris image acquired from a camera is localized by finding the center of pupil from the spectrum image. The outer iris boundary is detected by drawing concentric circles of different radii from the pupil center and the intensities lying over the perimeter of the circle are summed up. The annular region lying between pupil and iris boundary is transformed to polar co-ordinates to take into consideration the possibility of pupil dilation and appearing of different size in dif ferent images. From the normalized strip the eyelids are detected and removed.

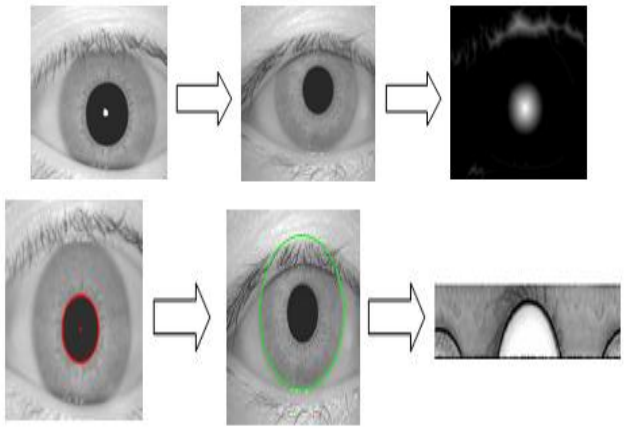

Fig 4: Steps involved in iris preprocessing and normalization

A. Feature Extraction using Haar Wavelet and Circular Mellin operator

- *Haar Wavelet*

Haar wavelet is widely used in texture recognition algorithms. The input signal *S* (polarized iris image) is decomposed into approximation, vertical, horizontal and diagonal coefficients using the wavelet transformation and coefficients for the fourth and fifth levels are chosen to reduce space complexity and discard the redundant information. The iris code is generated by assigning one to the positive coefficient values and zero to negative values.

- *Circular Mellin Operators*

These "Circular Mellin" operators are invariant to both scale and orientation of the target and represent the spectral decomposition of the image scene in the polar-log coordinate system. Features in iris images are extracted based on the phase of convolution of polarized iris image with mellin operators. The iris code is one for positive phase values and zero for negative phase values.The iris codes generated using Haar Wavelet and Circular Mellin operators are matched using Hamming Distance approach.

Combination of Haar Wavelet and Circular Mellin operatorThe individual matching scores generated by above mentioned classifiers are converted from distance to similarity score and are fused at matching score level for better performance of iris recognition.

B. Signature Verification

In biometrics terminology, the signature is a behavioral characteristic of a person and can be used to identify/verify a person's identity. The signature recognition algorithm consists of three major modules i.e., preprocessing and noise removal, feature extraction and computation of Euclidean distance. A scanned signature image may require morphological operations like normalization, noise removal by eliminating extra dots from the image, conversion to grayscale, thinning and extraction of high pressure region.

C. Feature Extraction using Global and Local feature:

The features of the signature images can be classified into two categories - global and local . Global features include the global characteristics of an image. Examples include: width/height (or length), baseline, area of black pixels etc. They are less responsive to small distortions and hence are less sensitive to noise as well, compared to local features which are confined to a limited portion of the signature. In contrast to global features, they are susceptible to small distortions like dirt but are not influenced by other regions of the signature. Hence, though extraction of local features requires a huge number of computations, they are much more precise. However, the grid size has to be chosen very carefully. Examples include local gradients, pixel distribution in local segments etc. Many of the global features such as global baseline, center of gravity, and distribution of black pixels have their local counterparts as well.The difference/distance (D_{Sign}) between the two feature sets are computed using weighted Euclidean distance measure.

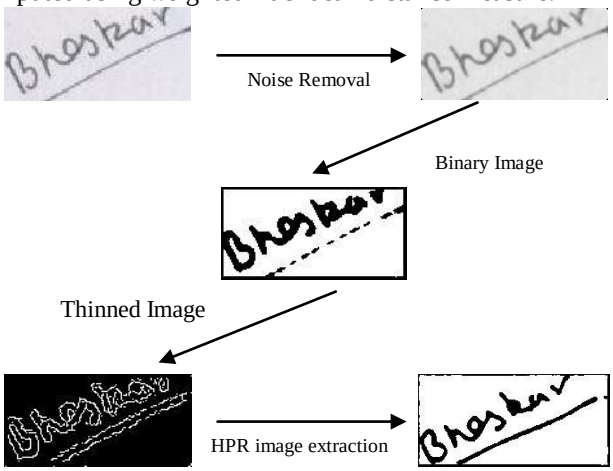

Fig 5: Preprocessing and noise removal

Fusion

Steps involved in fusion are as follows:

Step1: Given a query image as input, features are extracted by the individual recognizers and then an individual comparison algorithm for each recognizer compares the set of features and calculates the matching scores or distances corresponding to each recognizer for various traits.

Step2: The scores/distances obtained in S1 are normalized to a common range between 0 to 1.

Step3: These scores are then converted from distance to similarity score by subtraction from 1 if it is a dissimilarity score. For example the dissimilarity scores, in case of fingerprint recognition using reference point algorithm (D_{Ref}), iris recognition using Haar Wavelet (D_{Haar}) and Circular Mellin operator (D_{Mellin}) are converted to similarity scores (MS_{Ref}, MS_{Haar}, MS_{Mellin})

Step4: The matching scores are further rescaled so that threshold value becomes same for each recognizer.

Step5: Then the combined matching score is calculated by fusion of the matching scores of multiple classifiers using sum rule technique.

$$MS_{Face} = \frac{\alpha \times MS_{EBGM} + \beta \times MS_{KDDA}}{2},$$

$$MS_{Finger} = \frac{\alpha \times MS_{\mathrm{Re}f} + \beta \times MS_{MIN}}{2}$$

$$MS_{Iris} = \frac{\alpha \times MS_{Haar} + \beta \times MS_{Mellin}}{2}$$

where α and β are the weights assigned to individual classifiers. Currently equal weightage is given to each classifiers and the value of α and β is one.

The multimodal biometric system is developed by integrating four traits i.e., face, fingerprint, iris and signature at matching score level. Based on the proximity of feature vector and template, each subsystem computes its own matching score. These individual scores are finally combined into a total score, which is passed to the decision module. The matching scores are further rescaled so that the threshold value becomes common for all the subsystems. Finally, the sum of score technique is applied for combining the matching scores of four traits i.e., face, fingerprint, iris and signature.

Thus the final score MS_{Final} is given by,

$$MS_{Final} = \frac{1}{4}(\alpha \times MS_{Face} + b \times MS_{Finger} + c \times MS_{Iris} + d \times MS_{Sign})$$

where MS_{Face} = matching score of face, MS_{Finger} = matching score of fingerprint, MS_{Iris} = matching score of iris, and MS_{Sign} = matching score of signature and a, b, c and d are the weights assigned to the various traits. Currently, equal weightage is assigned to each trait so the value of a, b, c and d is one. The final matching score (MS_{Final}) is compared against a certain threshold value to recognize the person as genuine or an imposter.

VI. Conclusion

Biometrics systems are widely used to overcome the traditional methods of authentication. But the unimodal biometric system fails in case of lack of biometric data for particular trait. Thus the individual scores of four traits (face, fingerprint, iris and signature) are combined at classifier level and trait level to develop a multimodal biometric system. The performance table and accuracy curve shows that multimodal system performs better as compared to unimodal biometrics with accuracy of more than 97%. However, it is worth studying the results by assigning different weightage to different traits. At present equal weightage is assigned to each trait. Multimodal systems also provide anti-spoofing measures by making it difficult for an intruder to spoof multiple biometric traits simultaneously..

References

[1] L. Hong, A. Jain & S. Pankanti, Can Multibiometrics Improve performance, *Proceedings of* AutoID *99*, pp. 59-64, 1999.

[2] A. Ross & A. K. Jain, Information Fusion in Biometrics, Pattern Recognition Letters, 24 , pp. 2115-2125, 2003.

[3] W. Yunhong, T. Tan & A. K. Jain, Combining Face and Iris Biometrics for Identity Verification, Proceedings of Fourth International Conference on 2003

[4] Ravichandran & M. M. Trivedi, Circular-Mellin Features for Texture Segmentation, IEEE Transactions on Image Processing 4 Vol., pp. 1629-1640,1995.